REMARKS/ARGUMENTS

Claims 1-80 are pending in the present application.

This Amendment is in response to the final Office Action mailed January 11, 2005. In the final Office Action, the Examiner rejected claims 1-5, 20-25, 40-45, 60-65 and 80 under 35 U.S.C. §102(e); and claims 6-19, 26-39, 46-59, and 66-79 under 35 U.S.C. §103(a). Reconsideration in light of the remarks made herein is respectfully requested.

Rejection Under 35 U.S.C. § 102

1. In the Office Action, the Examiner rejected claims 1-5, 20-25, 40-45, 60-65 and 80 under 35 U.S.C. §102(e) as being anticipated U.S. Patent No. 6,327,652 issued to England et al. ("England"). Applicants respectfully traverse the rejection and contend that the Examiner has not met the burden of establishing a prima facie case of anticipation. To anticipate a claim, the reference must teach every element of a the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verregaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ 2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the...claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989).

England discloses loading and identifying a digital rights management operating system (DRMOS). Upon power up, a boot loader loads a boot block for a particular operating system. Code in the boot block then loads various drivers and other software components necessary for the OS to function on the computer (England, col. 11, lines 38-45). Once all components are loaded, the OS assumes its identity. A one-way hashing function provided by the CPU is used to create a cryptographic digest of all the loaded components. The digest becomes the identity for the OS (England, col. 12, lines 53-58). The DRMOS must provide a secure storage space to protect content permanently stored on the computer by securely storing private keys or session keys for use with encrypted content (England, col. 16, lines 50-55).

England does not disclose, either expressly or inherently, (1) a digest memory to store an isolated digest as recited in claims 1, 21, 41, and 61, (2) a device to attest the isolated execution mode and prove validity of a program loaded into the isolated memory area as recited in claims

1, 21, 41, and 61, (3) a secure environment for an isolated execution mode as recited in claims 1, 21, 41, and 61, (4) a processor operating in one of a normal execution mode and the isolated execution mode as recited in claims 1, 21, 41, and 61, (5) the isolated digest includes at least a digest of one of a processor nub loader, a processor nub, an operating system nub, and a supervisory module loaded in an isolated execution space as recited in claims 2, 22, 42, and 62, (6) an interface to map the device to an address space of a chipset in the secure environment as recited in claims 3, 23, 43, and 63, and (5) a communication storage to exchange security information with the processor in the isolated execution mode as recited in claims 3, 23, 43, and 63.

The Examiner states that the isolated execution mode is interpreted as a mode in which other applications or other unauthorized areas of memory cannot access (Final Office Action, page 3). The Examiner further states that the function of preventing access to a memory while a certain application is running can be interpreted as isolated execution mode because access is prohibited while the trusted application is running in the DRMOS (Final Office Action, page 3). Applicants respectfully disagree for the following reasons.

Claims should be interpreted consistently with the specification, which provides content for the proper construction of the claims because it explains the nature of the patentee's invention. See Renishaw P.L.C. v. Marposs Societa Per Azioni, 158 F.3d 1243 (Fed. Cir. 1998). During patent examination, the pending claims must be "given the broadest reasonable interpretation consistent with the specification". See MPEP 2111. Here, the isolated memory area and the isolated execution mode should be interpreted according to the specification, and not by an arbitrary interpretation.

England merely discloses creating identities for different versions of a digital right management operating system (DRMOS) (England, col. 11, lines 18-20). The totality of the boot block and the loaded components make up the identity of the operating system (England, col. 11, lines 44-46). England does not disclose an isolated memory area. England merely discloses checks the signature of a component before loading it (England, col. 11, lines 53-54). There is no distinction between an isolated memory area and a normal memory area.

In addition, England merely discloses using a one-way hashing function provided by the CPU to create a cryptographic digest of all the loaded components and use it as the identity of

the operating system (England, col. 12, lines 54-58). This is not the same as the digest memory that stores the digest values of the loaded processor nub, the operating system nub, and other supervisory modules loaded into the isolated execution space (See, for example, Specification, page 13, lines 21-24).

Furthermore, England merely discloses a CPU running in a normal mode, not in one of a normal execution mode and an isolated execution mode. When the computer is turned on, the CPU executes a boot loader to load a boot block for a particular operating system (England, col. 11, lines 38-42). In contrast, the isolated execution mode provides a secure environment to the platform. The security features are provided by a number of operations. The isolated execution mode is initialized using a privilege instruction and a processor nub loader (See, for example, Specification, page 7, lines 9-11). The isolated execution mode is supported by an isolated execution circuit including configuration for isolated execution, definition of an isolated area, definition (e.g., decoding and execution) of isolated instructions, etc. (See, for example, Specification, page 10, lines 7-13).

Therefore, Applicants believe that independent claims 1, 21, 41, 61 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicants respectfully request the rejection under 35 U.S.C. §102(e) be withdrawn.

Rejection Under 35 U.S.C. § 103

1. In the final Office Action, the Examiner rejected claims 6-19, 26-39, 46-59, and 66-79 under 35 U.S.C. §103(a) as being unpatentable over England in view of U.S. Patent No. 4,319,323 issued to Ermolovich ("Ermolovich"). Applicants respectfully traverse the rejection and contend that the Examiner has not met the burden of establishing a prima facie case of obviousness. To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *MPEP §2143, p. 2100-129 (8th Ed., rev. 2, May 2004).* Applicants respectfully

contends that there is no suggestion or motivation to combine their teachings, and thus no *prima facie* case of obviousness has been established.

England discloses loading and identifying a digital rights management operating system as discussed above.

Ermolovich discloses a communications device for data processing system. A device status is built and inserted into a packet as a status longword before inserting a command packet into a termination queue (Ermolovich, coo. 85, lines 37-41). The device status contains the status of a communication device after the communication device processes a command packet (Ermolovich, col. 13, lines 37-43). A command interpreter transfers contents of a command field to a command register in an external device (Ermolovich, col. 12, lines 2-6). The communication device may directly write to or read from buffers in the data block and command block (Ermolovich, col. 7, lines 54-58).

England and Ermolovich, taken alone or in any combination, do not disclose, suggest, or render obvious (1) a communication storage to exchange security information with the processor in the isolated execution mode, (2) a status register to store device status of the device, (3) a command register to store a device command for a command interface set; and (4) an input/output block (IOB) to store input and output data corresponding to the command.

There is no motivation to combine England and Ermolovich because neither of them addresses the problem of isolated execution. There is no teaching or suggestion that a digest memory, a device to attest isolated execution mode, and a processor having normal and isolated execution modes is present. England, read as a whole, does not suggest the desirability of attesting an isolated execution mode, or proving validity of a program, or a configuration storage in a communication storage corresponding to an address space for an isolated execution mode. England does not disclose or suggest an isolated execution mode as discussed above. Ermolovich merely discloses status word in a command packet for a communication device, not a configuration storage for an isolated execution mode. Ermolovich merely discloses a state to initiate a data transfer. In this state, a command interpreter is enabled to transfer the contents of the command field to a command register in the external device (Ermolovich, col. 12, lines 2-6). As noted above, the command register here is used only for communication devices and data transfers, not to allow the attestation key memory device to exchange security information with

at least one processor. The Examiner further states that Ermolovich discloses an input/output block to store input and output data and cites column 71, lines 40-64 (Final Office Action, page 6). However, the cited paragraph merely discloses a data block and command block which contain buffers to/from which the communication device directly writes/reads (Ermolovich, col. 71, lines 54-59). This is not the same as input and output data corresponding to the command used in exchanging security information and corresponding to an address space of a chipset in a secure environment.

The Examiner failed to establish a prima facie case of obviousness and failed to show there is teaching, suggestion or motivation to combine the references. "When determining the patentability of a claimed invention which combined two known elements, 'the question is whether there is something in the prior art as a whole suggest the desirability, and thus the obviousness, of making the combination.'" In re Beattie, Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co., 730 F.2d 1452, 1462, 221 USPQ (BNA) 481, 488 (Fed. Cir. 1984). "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or implicitly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 227 USPQ 972, 973. (Bd.Pat.App.&Inter. 1985).

In the present invention, the cited references do not expressly or implicitly suggest (1) a communication storage to exchange security information with the processor in the isolated execution mode, (2) a status register to store device status of the device, (3) a command register to store a device command for a command interface set; and (4) an input/output block (IOB) to store input and output data corresponding to the command. In addition, the Examiner failed to present a convincing line of reasoning as to why a combination of England and Ermolovich is an obvious application of attestation using an isolated digest and an isolated execution mode.

Therefore, Applicants believe that independent claims 6-19, 26-39, 46-59, and 66-79 are distinguishable over the cited prior art references. Accordingly, Applicants respectfully request the rejections under 35 U.S.C. §103(a) be withdrawn.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: February 28, 2005 By _____

Thinh V. Nguyen
Reg. No. 42,034
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: February 28, 2005

FACSIMILE

☒ *transmitted by facsimile to the Patent and Trademark Office.*

February 28, 2005

Tu Nguyen *Date*